WHAT IS CLAIMED IS:

Sub a3

1. An authentication system comprising:

a signing station which creates an authenticator by applying a one-way function to an information and then appends a signature generated from the authenticator to the information;

a certifying station for checking the authentication of the information from the authenticator included in the data received from said signing station;

wherein said signing station has,

a first authenticator creating unit for dividing the information into a plurality of data each having a prespecified length, and creating a plurality of authenticators by applying a different one-way function to each of the data; and

a linking unit for linking the plurality of authenticators created in said first authenticator creating unit to the information;

and said certifying station has,

a separating unit for separating the information and the plurality of authenticators from the data received from said signing station;

a second authenticator creating unit for dividing the information separated by said separating unit into a plurality of data each having a prespecified length, and creating a plurality of authenticators by applying a different one-way function to each of the data; and

a certifying unit for comparing the plurality of authenticators created by said second authenticator creating unit with the plurality of authenticators separated from the information by said separating unit, and checking the authentication of the information.

2. An authentication system according to Claim 1; wherein said linking unit links the authenticators obtained by truncating the authenticators created by said first authenticator creating unit to the information, and

said certifying unit compares the authenticators obtained by truncating the authenticators created by said second authenticator creating unit to the authenticators separated from the information by said separating unit and checking the authentication of the information.

3. An authentication system according to Claim 2; wherein said first authenticator creating unit and said second authenticator creating unit create a first authenticator by subjecting a first data to a one-way operation using a first key, and prepare a second authenticator by subjecting a second data to a one-way operation using a second key.

4. An authentication system according to Claim 3; wherein each of said first authenticator creating unit and said second authenticator creating unit discretely and independently creates the first authenticator and the second authenticator in parallel with each other.

5. An authentication system according to Claim 3; wherein each of said first authenticator creating unit and said second authenticator creating unit utilize an intermediate data when creating the second authenticator, which intermediate data is generated when the first authenticator is created.

6. An authentication method applied in an authentication system, wherein said authentication system has a signing station which creates an authenticator by applying a one-way function to an information and then appends a signature generated from the authenticator to the information, and a certifying station for checking the authentication of the information from the authenticator included in the data received from said signing station; wherein

said signing station executes,

a first authenticator creating step of dividing the information into a plurality of data each having a prespecified length, and creating a plurality of authenticators by applying a different one-way function to each of the data; and a transmitting step of linking the plurality of authenticators created in said first authenticator creating step to the information and transmitting the information to the certifying station; and

said certifying station executes,

a separating step of separating the information and the plurality of authenticators from the data received from said signing station;

a second authenticator creating step of dividing the information separated in said separating step into a plurality of data each having a prespecified length, and creating a plurality of authenticators by applying a different one-way function to each of the data; and

a certifying step of comparing the plurality of authenticators created in said second authenticator creating step with the plurality of authenticators separated from the information in said separating step, and checking the authentication of the information.

7. An authentication method according to Claim 6; wherein said transmitting step comprises a step of linking the authenticators obtained by truncating the authenticators created in said first authenticator creating step to the information, and

said certifying step comprises a step of comparing the authenticator obtained by truncating the authenticators created in said second authenticator creating step to the authenticators separated from the information in said separating step and a step of checking the authentication of the information.

8. An authentication method according to Claim 7; wherein said first authenticator creating step and said second authenticator creating step comprise a step of creating a first authenticator by subjecting a first data to a one-way operation using a first key, and a step of creating a second authenticator by subjecting a second data to a one-way operation using a second key.

9. An authentication method according to Claim 8; wherein each of said first authenticator creating step and said second authenticator creating step comprise a step of discretely and independently creating the first authenticator and the second authenticator in parallel with each other.

10. An authentication system according to Claim 8; wherein each of said first authenticator creating step and said second authenticator creating step comprise a step of utilizing an intermediate data when creating the second authenticator, which intermediate data is generated when the first authenticator is

created.

11. A computer-readable recording medium with a program recorded therein for making a computer execute the authentication method applied in an authentication system, wherein said authentication system has a signing station which creates an authenticator by applying a one-way function to an information and then appends a signature generated from the authenticator to the information, and a certifying station for checking the authentication of the information from the authenticator included in the data received from said signing station; wherein

the program makes said signing station execute,

a first authenticator creating step of dividing the information into a plurality of data each having a prespecified length, and creating a plurality of authenticators by applying a different one-way function to each of the data; and

a transmitting step of linking the plurality of authenticators created in said first authenticator creating step to the information and transmitting the information to the certifying station; and

the program makes said certifying station execute,

a separating step of separating the information and the plurality of authenticators from the data received from said signing station;

a second authenticator creating step of dividing the information separated in said separating step into a plurality of data each having a prespecified length, and creating a plurality of authenticators by applying a different one-way function to each of the data; and

a certifying step of comparing the plurality of authenticators created in said second authenticator creating step with the plurality of authenticators separated from the information in said separating step, and checking the authentication of the information.

12. A signing apparatus which creates an authenticator by utilizing a key and applying a one-way function to an information and then appends a signature to the information; said apparatus comprising:

a dividing unit for dividing the information into a plurality of data;

an authenticator creating unit for creating an authenticator by utilizing a key and applying a one-way function corresponding to each of the divided data; and

a linking unit for linking the plurality of created authenticators to the information.

13. A signing apparatus which creates an authenticator by utilizing a key and applying a one-way function to an information and then appends a signature to the information; said apparatus comprising:

a dividing unit for dividing the information into a plurality of data;

an authenticator creating unit for repeating the creation of an authenticator by utilizing a key and applying a one-way function to one of the divided data as well as creation of an authenticator by utilizing a key and applying a one-way function to a desired intermediate data the next data when the one-way function was applied.

a linking unit for linking the plurality of created authenticators to the information.

14. A certifying apparatus which creates an authenticator by utilizing a key and applying a one-way function to an information and then appends a signature to the information as well as checks the authentication of the information; said apparatus comprising:

a separating unit for separating information and the plurality of authenticators from the data;

a dividing unit for dividing the information into a plurality of data;

an authenticator creating unit for creating an authenticators by utilizing a key and applying a one-way function corresponding to each of the divided data; and

a certifying unit for checking the authentication of the information based on each of the created authenticators and each of the separated authenticators.

15. A certifying apparatus which creates an authenticator by utilizing a key and applying a one-way function to an information and then appends a signature to the information as well as checks the authentication of the information; said apparatus comprising:

a separating unit for separating information and the plurality of authenticators from the data;

a dividing unit for dividing the information into a plurality of data;

an authenticator creating unit for repeating the creation of an authenticator by utilizing a key and applying a one-way function to one of the divided data as well as creation of an authenticator by utilizing a key and applying a one-way function to a desired intermediate data the next data when the one-way function was applied; and

a certifying unit for checking the authentication of the information based on each of the created authenticators and each of the separated authenticators.

16. A computer-readable recording medium with a program recorded therein for making a computer execute:

a dividing step of dividing an information into a plurality of data;

an authenticator creating step of creating an authenticator by utilizing a key and applying a one-way function corresponding to each of the divided data; and

a linking step of linking the plurality of created authenticators to the information.

17. A computer-readable recording medium with a program recorded therein for making a computer execute:

a dividing step of dividing an information into a plurality of data;

an authenticator creating step of repeating the creation of an authenticator by utilizing a key and applying a one-way function to one of the divided data as well as creation of an authenticator by utilizing a key and applying a one-way function to a desired intermediate data the next data when the one-way function was applied; and

a linking step of linking the plurality of created authenticators to the information.

18. A computer-readable recording medium with a program recorded therein for making a computer execute:

a separating step of separating information and a plurality of authenticators from the data;

a dividing step of dividing the information into a plurality of data;

an authenticator creating step of creating an authenticators by utilizing a key and applying a one-way function corresponding to each of the divided data; and

a certifying step of checking the authentication of the information based on each of the created authenticators and each of the separated authenticators.

19. A computer-readable recording medium with a program recorded therein for making a computer execute:

a separating step of separating information and plurality of authenticators from a data;

a dividing step of dividing the information into a plurality of data;

an authenticator creating step of repeating the creation of an authenticator by utilizing a key and applying a one-way function to one of the divided data as well as creation of an authenticator by utilizing a key and applying a one-way function to a desired intermediate data the next data when the one-way function was applied; and a certifying step of checking the authentication of the information based on each of the created authenticators and each of the separated authenticators.

20. A signing method in which an authenticator is created by utilizing a key and applying a one-way function to an information and then a signature is appended to the information; said method comprising:

a dividing step of dividing an information into a plurality of data;

an authenticator creating step of creating an authenticator by utilizing a key and applying a one-way function corresponding to each of the divided data; and

a linking step of linking the plurality of created authenticators to the information.

21. A signing method in which an authenticator is created by utilizing a key and applying a one-way function to an information and then a signature is appended to the information; said method comprising:

a dividing step of dividing an information into a plurality of data;

an authenticator creating step of repeating the creation of an authenticator by utilizing a key and applying a one-way function to one of the divided data as well as creation of an authenticator by utilizing a key and applying a one-way function to a desired intermediate data the next data when the one-way function was applied; and

a linking step of linking the plurality of created authenticators to the information.

22. A certifying method in which an authenticator is created by utilizing a key and applying a one-way function to an information and then a signature is appended to the information as well as the authentication of the information is checked; said method comprising:

a separating step of separating information and a plurality of authenticators from the data;

a dividing step of dividing the information into a plurality of data;

an authenticator creating step of creating an authenticators by utilizing a key and applying a one-way function corresponding to each of the divided data; and

a certifying step of checking the authentication of the information based on each of the created authenticators and each of the separated authenticators.

23. A certifying method in which an authenticator is created by utilizing a key and applying a one-way function to an information and then a signature is appended to the information

as well as the authentication of the information is checked; said method comprising:

a separating step of separating information and plurality of authenticators from a data;

a dividing step of dividing the information into a plurality of data;

an authenticator creating step of repeating the creation of an authenticator by utilizing a key and applying a one-way function to one of the divided data as well as creation of an authenticator by utilizing a key and applying a one-way function to a desired intermediate data the next data when the one-way function was applied; and

a certifying step of checking the authentication of the information based on each of the created authenticators and each of the separated authenticators.